水利署臺北水源特定區管理分署
資訊資產暨風險評鑑表

資通系統(服務)名稱：
安全等級：
業務屬性：
科室名稱：
資通系統(服務)負責人：
科室主管：

項次	資訊資產名稱	管理人	資訊資產說明	存放位置	資產類別	數量	機密性	完整性	可用性	資訊資產價值	威脅	脆弱性	安控前				風險降低原因說明	安控後			
													威脅等級	脆弱等級	風險值	風險等級		威脅等級	脆弱等級	風險值	風險等級

資訊紀錄	電腦系統	實體設備
火災_IA	入侵_CIA	水災_IA
未授權存取資料_CI	阻斷服務攻擊_IA	火災_IA
作業人員或使用者錯誤_I	未授權軟體變更_I	未授權存取資料_CI
作業失能_IA	未授權撥接存取_CI	地震_IA
委外作業失能_IA	作業人員或使用者錯誤_I	有害動物_IA
社交工程_C	技術失能_IA	污染_A
冒充_CIA	使用盜版軟體_I	污染放射線_A
破壞_IA	委外作業失能_IA	作業人員或使用者錯誤_I
竊聽_C	社交工程_C	技術失能_IA
偷竊_CI	破壞_IA	委外作業失能_IA
軟體程式錯誤_I	軟體程式錯誤_IA	破壞_IA
通訊失能_A	惡意程式碼_CIA	偷竊_CIA
惡意破壞資料與設施_IA		通訊服務失能_A
惡意程式碼_CIA		惡意破壞資料與設施_IA
詐欺_CI		極端的溫濕度_A
傳輸錯誤_I		電力供給失能_A
資料外洩_C		電子干擾_A
誤傳_I		電源不穩_A
竄改或任意變更_I		暴風雨_A

服務	人員
干擾_A	未授權存取資料_CI
中斷_A	罷工_A
誤用_IA	未授權軟體變更_I
	作業人員或使用者錯誤_I
	否認_I
	使用盜版軟體_I
	委外作業失能_IA
	社交工程_C
	破壞_IA
	偷竊_CIA
	詐欺_CI
	誤傳_I
	竄改或任意變更_I
	請假_A
	離職或更換頻繁_A

資訊紀錄_火災_IA	資訊紀錄_未授權存取資料_CI
使用易燃性之材質，如紙或盒子。	網路存取規劃不當。 非單位內人員進出未有適當人員陪同。 缺少實體安控。 對有計畫的破壞行動缺乏懲戒處分。 軟體開發者與作業人員的職責未釐清。 程式人員監督不週。

資訊紀錄_作業人員或使用者錯誤_I	資訊紀錄_作業失能_IA
安全訓練不足。	備份失效
使用者認知不足。	保存不當
缺少文件。	
缺少有效的型態管理控制。	
複雜的使用者介面。	

資訊紀錄_委外作業失能_IA	資訊紀錄_社交工程_C
未釐清委外協議的權責。	缺少要求同仁不可在電話上提供資訊的規範。 缺少資訊諮詢的規範：待釐清詢問者的身份再給予資訊。

資訊紀錄_冒充_CIA	資訊紀錄_破壞_IA
未保護通行碼(password)檔。	存取權限不對。
缺乏身份鑑別與辨識機制。	缺少實體安控。
通行碼易被人識破/取得。	缺少變更管理控制。
	缺少邏輯上(技術或系統)的存取安控。
	對有計畫的破壞行動缺乏懲戒處分。

資訊紀錄_竊聽_C

未規範行動與遠端裝置之使用。

使用分享的乙太網路意即訊號會廣播到區域網路中之每一部機器。

缺乏交換資訊協議。

通訊未加密。

資料通訊室或中心缺少實體安控。

資訊紀錄_偷竊_CI	資訊紀錄_軟體程式錯誤_I
未控制資料及/或軟體複製。	不清楚或不完整之開發規格。 技術不足的人員。 系統發展生命週期程序不足。 缺少有效的型態管理控制。

資訊紀錄_通訊失能_A	資訊紀錄_惡意破壞資料與設施_IA
未規劃與建置通訊線路。	缺少實體安控。
缺少備援與備份設備。	缺少邏輯上(技術或系統)的存取安控。
缺乏意外處理機制。	缺乏溝通導致離職同仁可存取系統。
	對有計畫的破壞行動缺乏懲戒處分。

資訊紀錄_惡意程式碼_CIA	資訊紀錄_詐欺_CI
未定期更新防毒軟體(病毒碼及掃瞄引擎)。	缺乏應用系統控管導致不實的付款。
未規劃與建置通訊線路。	
沒有防毒軟體。	
對人員在軟體病毒的教育不足。	
未實施程式碼檢驗。	
對有計畫的破壞行動缺乏懲戒處分。	

資訊紀錄_傳輸錯誤_I	資訊紀錄_資料外洩_C
佈線不當。 缺乏意外處理機制。	資料分級錯誤或處理不當。

資訊紀錄_誤傳_I
使用者訓練不足。
缺少接收訊息證明。
傳輸機密資料未加適當防護。

資訊紀錄_竄改或任意變更_I

缺少實體安控。

缺少邏輯上(技術或系統)的存取安控。

缺乏加解密規範與控管機制。

缺乏有效的變更管理。

電腦系統_入侵_CIA	電腦系統_阻斷服務攻擊_IA
未更新或安裝作業系統/軟體的修補程式。	網路管理不足。
開發或設定標準不足。	缺乏備援系統。

電腦系統_未授權軟體變更_I	電腦系統_未授權撥接存取_CI
缺少軟體變更管理規範與程序。 缺少備份。 缺少變更管理軟體。 軟體失能的處理或報告不恰當。 軟體開發者與作業人員的職責未釐清。 程式人員監督不週。	缺少使用者身份辨識。

電腦系統_作業人員或使用者錯誤_I	電腦系統_技術失能_IA	電腦系統_使用盜版軟體_I
使用者認知不足。 缺少有效的型態管理控制。	使用者認知不足。 變更管理流程失誤。 缺乏原始碼無法修改程式	未限制複製軟體。 缺少人員使用合法軟體的規範。 缺少軟體稽核。 軟體派送安裝機制不足。

電腦系統_委外作業失能_IA	電腦系統_社交工程_C
未釐清委外協議的權責。	缺少要求同仁不可在電話上提供資訊的規範。 缺少資訊諮詢的規範：待釐清詢問者的身份再給予資訊。

電腦系統_破壞_IA	電腦系統_軟體程式錯誤_IA
存取權限不對。	不清楚或不完整之開發規格。
缺少變更管理控制。	技術不足的人員。
	系統發展生命週期程序不足。
	缺少有效的型態管理控制。

電腦系統_惡意程式碼_CIA	實體設備_水災_IA
未定期更新防毒軟體(病毒碼及掃瞄引擎)。	位於易有天然災害地區。
未控制由網際網路下載及使用軟體。	沒有回復資訊與資訊資產的營運持續管理與程序。
沒有防毒軟體。	備份檔案或系統無法使用。
資通安全政策不足。	

實體設備_火災_IA	實體設備_未授權存取資料_CI
位於易有天然災害地區。 沒有回復資訊與資訊資產的營運持續管理與程序。 使用易燃性之材質，如紙或盒子。 缺少火災偵測設備。 缺少自動滅火系統。 缺少實體安控。 備份檔案或系統無法使用。	缺少實體安控。 對有計畫的破壞行動缺乏懲戒處分。

實體設備_地震_IA
位於易有天然災害地區。
沒有回復資訊與資訊資產的營運持續管理與程序。
備份檔案或系統無法使用。

實體設備_有害動物(蟲、鳥、獸)_IA
位於易受環境影響的地區。
沒有回復資訊與資訊資產的營運持續管理與程序。

實體設備_污染_A	實體設備_污染(放射線)_A
位於易受環境影響的地區。	設備與設施缺乏維護。
沒有回復資訊與資訊資產的營運持續管理與程序。	備份檔案或系統無法使用。

實體設備_作業人員或使用者錯誤_I	實體設備_技術失能_IA
使用者認知不足。	由於不當的規劃或維護而導致網路容量不夠。 技術設施維護不恰當。 沒有回復資訊與資訊資產的營運持續管理與程序。 使用者認知不足。 缺少備份設施或流程。 缺乏環境保護。 變更管理流程失誤。

實體設備_委外作業失能_IA	實體設備_破壞_IA
沒有回復資訊與資訊資產的營運持續管理與程序。 備份檔案或系統無法使用。	缺少實體安控。 對有計畫的破壞行動缺乏懲戒處分。

實體設備_偷竊_CIA	實體設備_通訊服務失能_A	實體設備_惡意破壞資料與設施_IA
缺少實體安控。	網路管理不足(路徑彈性)。	缺少實體安控。 缺乏溝通導致離職同仁可存取系統。 對有計畫的破壞行動缺乏懲戒處分。

實體設備_極端的溫濕度_A	實體設備_電力供給失能_A
位於易受環境影響的地區。 沒有回復資訊與資訊資產的營運持續管理與程序。 環境監控不足。	電力供應設備容量不足。

實體設備_電子干擾_A
位於易受環境影響的地區。
沒有回復資訊與資訊資產的營運持續管理與程序。

實體設備_電源不穩_A

位於易有電源不穩定地區。

沒有回復資訊與資訊資產的營運持續管理與程序。

沒有電力調節設備。

實體設備_暴風雨(土石流,颱風)_A	服務_干擾_A
位於易有天然災害地區。 沒有回復資訊與資訊資產的營運持續管理與程序。	傳輸介面易遭破壞或干擾。

服務_中斷_A	服務_誤用_IA	人員_未授權存取資料_CI
缺乏應變計劃。	缺乏線路圖或標示不明。	未規劃與建置通訊線路。
容量不足。	未釐清委外協議的權責。	非單位內人員進出未有適當人員陪同。
未釐清委外協議的權責。	缺乏使用規範。	缺少實體安控。
維護不當。		傳輸機密資料未加適當防護。
		對有計畫的破壞行動缺乏懲戒處分。

人員_罷工_A	人員_未授權軟體變更_I
沒有回復資訊與資訊資產的營運持續管理與程序。 缺乏勞資協議。	缺少接收訊息證明。 缺少軟體變更管理規範與程序。 缺少備份。 軟體失能的處理或報告不恰當。 軟體開發者與作業人員的職責未釐清。 程式人員監督不週。 傳輸機密資料未加適當防護。

人員_作業人員或使用者錯誤_I	人員_否認_I	人員_使用盜版軟體_I
安全訓練不足。	未使用數位簽章。	未限制複製軟體。
使用者認知不足。	缺少收送訊息證明。	
缺少文件。		
缺少有效的型態管理控制。		
複雜的使用者介面。		

人員_委外作業失能_IA	人員_社交工程_C
未釐清委外協議的權責。	使用分享的乙太網路意即訊號會廣播到區域網路中之每一部機器。 缺少要求同仁不可在電話上提供資訊的規範。 缺少資訊諮詢的規範：待釐清詢問者的身份再給予資訊。 缺乏交換資訊協議。 通訊未加密。 資訊相關辦公室或機房缺少實體安控。 對有計畫的破壞行動缺乏懲戒處分。

人員_破壞(偷竊,詐欺,竄改)_IA	人員_偷竊_CIA
對有計畫的破壞行動缺乏懲戒處分。	未控制資料及/或軟體複製。

人員_詐欺_CI	人員_誤傳_I
缺乏應用系統控管導致不實的付款。	使用者訓練不足。 缺少接收訊息證明。 傳輸機密資料未加適當防護。

人員_竄改或任意變更_I	人員_請假_A
缺少實體安控。	缺乏職務代理能力
缺少邏輯上(技術或系統)的存取安控。	缺乏標準作業程序
缺乏加解密規範與控管機制。	
缺乏有效的軟體變更管理導致未授權軟體變更而製造詐欺事件。	

人員_離職或更換頻繁_A
交接資料不足或未建立
缺乏標準作業程序

風險最大值	風險最小值	風險等級值
27	1	

6
12
27